Q & A's
The *Freedom of Information and Protection of Privacy Amendment Act, 2004*: A Response to the USA Patriot Act

1. How and why does the USA Patriot Act impact British Columbians?

The USA Patriot Act (Patriot Act) is law passed by the American government in response to concerns about international crime and terrorism that were brought to the forefront by the catastrophic events of September 11, 2001. Section 215 of the Patriot Act allows the FBI to conduct electronic surveillance, enter a facility, or access business records of any American organization on a covert basis. Since many Canadian governments and corporations do business with American companies, those American companies or their affiliated associates may either hold or have access to the personal information of Canadians. Thus an FBI investigation under the authority of an order issued pursuant to s. 215 of the Patriot Act would potentially capture this information and expose British Columbians to scrutiny by the American government. The risk of this occurring, however, is small and incremental. There are existing legal mechanisms, such as treaties and other inter-jurisdictional agreements, that govern the sharing of this type of information, and it is unlikely that a US court would issue an order against a Canadian company simply because the company has American connections.

2. What is the BC Government's response to the USA Patriot Act?

British Columbia has the strongest privacy protection legislation in Canada. To ensure that this protection continues in the face of the Patriot Act, the BC Government has passed legislative amendments to the *Freedom of Information and Protection of Privacy Act* that strengthen the privacy protections already in place. The amendments are set out in the *Freedom of Information and Protection of Privacy Amendment Act*. In addition, government has developed a tool kit of contractual, business, employee and technical mechanisms to work in conjunction with the amendments to ensure that all avenues of unauthorized access have been addressed.

3. What does the new *Freedom of Information and Protection of Privacy Amendment* Act (FOIPP Amendment Act) do?

The FOIPP Amendment Act strengthens the privacy protections of the *Freedom of Information and Protection of Privacy Act* (1992) by adding provisions that:

- Prevent the storage and disclosure of, and access to, personal information outside of Canada by a service provider;

- Require service providers to report to government any requests for unauthorized access to personal information received from jurisdictions outside Canada;
- Create offences and penalties for violation of the disclosure, storage and access rules and for failing to report disclosures; and
- Provide protection for "whistle-blowers" who report violations of disclosure rules.

4. What should I do to ensure my ministry or public body is compliant with these new provisions?

- Download and review the FOIPP Amendment Act and other training and educational materials and tools on the Ministry of Management Services, Information Policy and Privacy Branch (IPPB) web site at: http://www.mser.gov.bc.ca/FOI_POP/index.htm.
- Review your ministry's or public body's existing compliance with the FOIPP Act with respect to outsourcing with contractors and other service providers, and identify the areas that need to be upgraded or modified to bring your policies and practices into compliance with the new provisions of the FOIPP Amendment Act.
- Contact the IPPB directly to ask specific questions or to request a meeting or briefing session that can provide you and your colleagues with more detailed information and advice about the new provisions: (250) 356-6228 or cpiaadmin@gems5.gov.bc.ca.

5. Are there any additional privacy protection measures that government recommends I implement to assist my ministry or public body in complying with the new provisions?

Yes. Although the new legislative provisions are the first and most uniform step towards securing and enhancing BC's existing privacy protections, government has also developed an additional set of "privacy protection measures" for public bodies to use to protect privacy. These measures are designed to:

- Limit the application of extraterritorial provisions in foreign legislation (such as the Patriot Act);
- Restrict the ability of a US company to compel disclosure;
- Ensure advance notice to the BC government of potential disclosure that is not authorized by BC's FOIPP Act or FOIPP Amendment Act; and
- Apply specific incentives and consequences to prevent disclosure.

6. What are these enhanced privacy protection measures and how do I apply them?

The enhanced protections are designed to be applied on a case-by-case basis, depending on the sensitivity of the personal information at issue. Many of these

protections may already be in place in your public body. These mechanisms mostly employ existing technology, business processes, corporate structures, employee strategies, and contractual measures that keep sensitive personal information from being inappropriately accessed.

For example, public bodies can proactively:

- Ensure that there are detailed privacy and security standards included in each contract;
- Complete a detailed Privacy Impact Assessment (PIA) for every project before proceeding to the development stage;
- Limit the contractor's employees' access to personal information;
- Incorporate audit trails and tracing mechanisms for employees accessing personal information;
- Require various levels of security clearances to access data;
- Contract only with non-US based subsidiaries (which effectively severs the link between personal information and the jurisdiction of the Patriot Act);
- Require that personal information be kept in Canada; and
- Incorporate termination rights into the contract whereby unauthorized disclosure results in termination of the contract.

It is important to note that this list is not exhaustive. The corporate relationship and its contractual obligations can be tailored to limit access to personal information and to identify offences and penalties.

7. Will all types of government contracts be affected by the new provisions and the enhanced privacy protection measures?

No. The only contracts affected are the **ones containing personal information**. The FOIPP Amendment Act defines personal information as "information about an identified individual other than contact information". Contact information is the name, phone or fax number, e-mail address etc. that enables an individual at a place of business to be contacted. Thus, if a ministry or other public body has a database containing the names of service providers, this information is limited to business contact information, and a contract to outsource the management of this database would not be impacted by the amendments.

Additionally, if a ministry or other public body is contracting with a local service provider that has no affiliation with other companies based outside of Canada, many of the new amendments and privacy protection measures will not apply because no foreign affiliation is involved. For example, if the Ministry of Children and Family Development is contracting with foster parents to care for children in BC, these foster parents likely do not subcontract with service providers based in another

country for functions involving the use of personal information, such as the management of case files. These contracts, therefore, are unlikely to be impacted by the new provisions.

8. What about existing contracts or legally binding agreements to contract? Are they grandfathered?

The FOIPP Amendment Act specifically addresses the issue of existing contracts with "transitional provisions". These provisions state that:

- If **government** entered into a contract **on or before October 12, 2004**, the contract is **not** subject to the new privacy protection provisions;
- If **government** became "legally obligated" to enter into a contract as a result of a completed, binding, competitive process **on or before October 12, 2004**, then the resulting contract is **not** subject to the new privacy protection provisions;
- If any **other public body** (such as a Crown corporation, municipality, or hospital) entered into a contract or became legally obligated to enter into a contract **on or before October 21, 2004** (the date the Bill received Royal Assent), then the new privacy protection provisions do **not** apply.

It is important to note, however, that the transitional provisions only have effect until the **end of the current term** of the existing or pending contract, and only where the government or other public body cannot reasonably bring the existing or pending contract into compliance with the new privacy protection provisions. Further, wherever possible, a public body **must make all reasonable efforts** to bring the contract into compliance with the provisions **despite** it not yet being covered by them. Finally, once the term of a current contract comes to an end, the new provisions **will** apply.

It is also important to note that the transitional provisions **do not apply to the new whistle-blower protections** of the FOIPP Amendment Act. Whistle-blower protection takes effect as of October 21, 2004 (the day of Royal Assent).

9. Who should I consult with to make sure I implement the FOIPP Amendment Act provisions correctly?

It is important that you include the following groups in your policy review and implementation plan:

- Your ministry or agency's Directors or Managers of Information and Privacy (DMIPS). They have the most in-depth knowledge about information and privacy requirements in your public body and know with whom to consult for further advice or access to resources;
- The Information Policy and Privacy Branch (IPPB) of the Ministry of Management Services for detailed information about the proposed amendments to the FOIPP Act and the enhanced privacy protection measures;

- The Alternative Service Delivery Secretariat (ASD) of the Ministry of Management Services for strategic contract assistance and detailed information about the ASD process;
- The Procurement Governance Office of the Ministry of Finance for Policy Assistance;
- The Strategic Acquisitions and Intellectual Property Management (SAIP) office of the Ministry of Management Services for detailed information about the RFP/contract process; and
- Your ministry solicitor about any legal issues that might arise, including contract language, altering competitive processes, and information on the incorporation or jurisdiction of contractors.